

# CUMA OS Password Reset Fails with the "pwrecovery" Process

Document ID: 112908

## Contents

### Introduction

#### Prerequisites

- Requirements

- Components Used

- Conventions

#### Problem

- Solution 1

- Solution 2

### Related Information

## Introduction

Cisco Unified Mobility Advantage (CUMA) is part of the Cisco Unified Communications family of products. CUMA is a server software deployed behind your enterprise firewall that connects employees' mobile phones to your directory servers, IP Communications system, groupware, and conferencing servers as well as other company resources. This extends critical business communications capabilities to mobile handsets and allows everyone to communicate more effectively.

This document provides the guidelines to troubleshoot the password recovery in the Cisco Unified Mobility Advantage Server.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on the CUMA server version 7.1.2.3.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

## Problem

The issue is you cannot log in with SSH or CLI, or Platform page. The pwrecovery procedure has been tried, but you still cannot login to the console. If an unacceptable password is entered during a pwrecovery, the

password is not usable. There are at least three types of passwords that are not accepted during a password reset:

- Password is too short
- Passwords do not match
- Password in dictionary

**Note:** If any of these types are used, an error is displayed. Then if a correct password is entered, it appears the password has been reset. However, the password is not usable. Any attempt to do a password recovery will not work in this case. You will be unable to login to the platform GUI or CLI.

## Solution 1

If you do not remember the admin password, here is the procedure to reset it. There are two methods to reset the password. The first one is without using a recovery CD and the other is with a CD.

1. Login to the linux box with the root account (this is a standard linux box).
2. Make sure these services are running:
  - ◆ /sbin/service cuma\_db start
  - ◆ /sbin/service cuma\_admin start
  - ◆ /sbin/service cuma\_nm start
3. Edit the file using vi editor: **/opt/cuma/conf/admin/admin.xml**.
4. Find this line:

```
<name>admin_password</name>  
  
<value>{MD5}xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx</value>
```

And change it to:

```
<name>admin_password</name>  
  
<value>{plain}new_password</value>
```

5. Use this command in order to restart the service:

```
/sbin/service cuma_admin restart
```

6. Login with "admin" and the "new\_password".

## Solution 2

The issue is you cannot reset the OS Admin Password when using the **pwrecovery** process. Complete these steps in order to resolve the issue:

1. Boot the system with the recovery CD (7.1.2 or later is recommended).
2. Make sure it can detect installation (that is printed with the main menu of recovery CD).
3. Press **alt+F2** to get access to the recovery CD's root shell.
4. Active partition should be on **/mnt/part1**. Make sure it is mounted properly.
5. Run the **chroot /mnt/part1 rpm -q master** and **chroot /mnt/part2 rpm -q master** commands in order to find the active partition.
6. After you run these commands and find the working version of the server from the returned results, you need to use it as the working partition.
7. Enter the active partition by **chroot /mnt/part1**, if it is a new installation.
8. If the server has been upgraded, use that specific part number (**chroot /mnt/part<no>**).


9. On earlier releases, run **/root/.security/unimmunize.sh** to remove the immutable bit from **/etc/passwd**.
10. Edit **/etc/passwd** and change **root:x:0:0:root:/root:/sbin/nologin** to **root:x:0:0:root:/root:/bin/bash**, then save the changes.
11. Run the **passwd root** command and give a password at the prompt, then confirm. Now you will have root access when you boot into the active partition.
12. Press **Alt+F1** to get the main recovery CD menu and enter **q** to quit. Then, eject the cd.
13. Press **ctrl+alt+delete** to reboot.
14. After this, **SSH** in as root and set a temporary password for the OS admin with this command: **passwd admin**, where admin is your OS Administrator's user login name.

**Note:** Here, the password is only used temporarily. You will need to do it again.

15. Start up the CLI with the **su – admin** command, where admin is the OS Administrator's login name.
16. Change the password in the database with the **set password user <admin id>** CLI command.
17. Exit from the CLI.
18. Set the OS Administrator's system password to match the database password with this command: **passwd admin**, where admin is the OS Administrator's login name.

**Note:** This is documented by Cisco bug ID CSCtf25554 (registered customers only) .

## Related Information

- [Using the Configuration Wizard in Cisco Unified Mobility Advantage](#)
- [Cisco Unified Mobility Advantage Server Certificate Issue with ASA](#)
- [Voice Technology Support](#)
- [Voice and Unified Communications Product Support](#)
- [Troubleshooting Cisco IP Telephony](#) 
- [Technical Support & Documentation – Cisco Systems](#)

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: May 13, 2011

Document ID: 112908

---